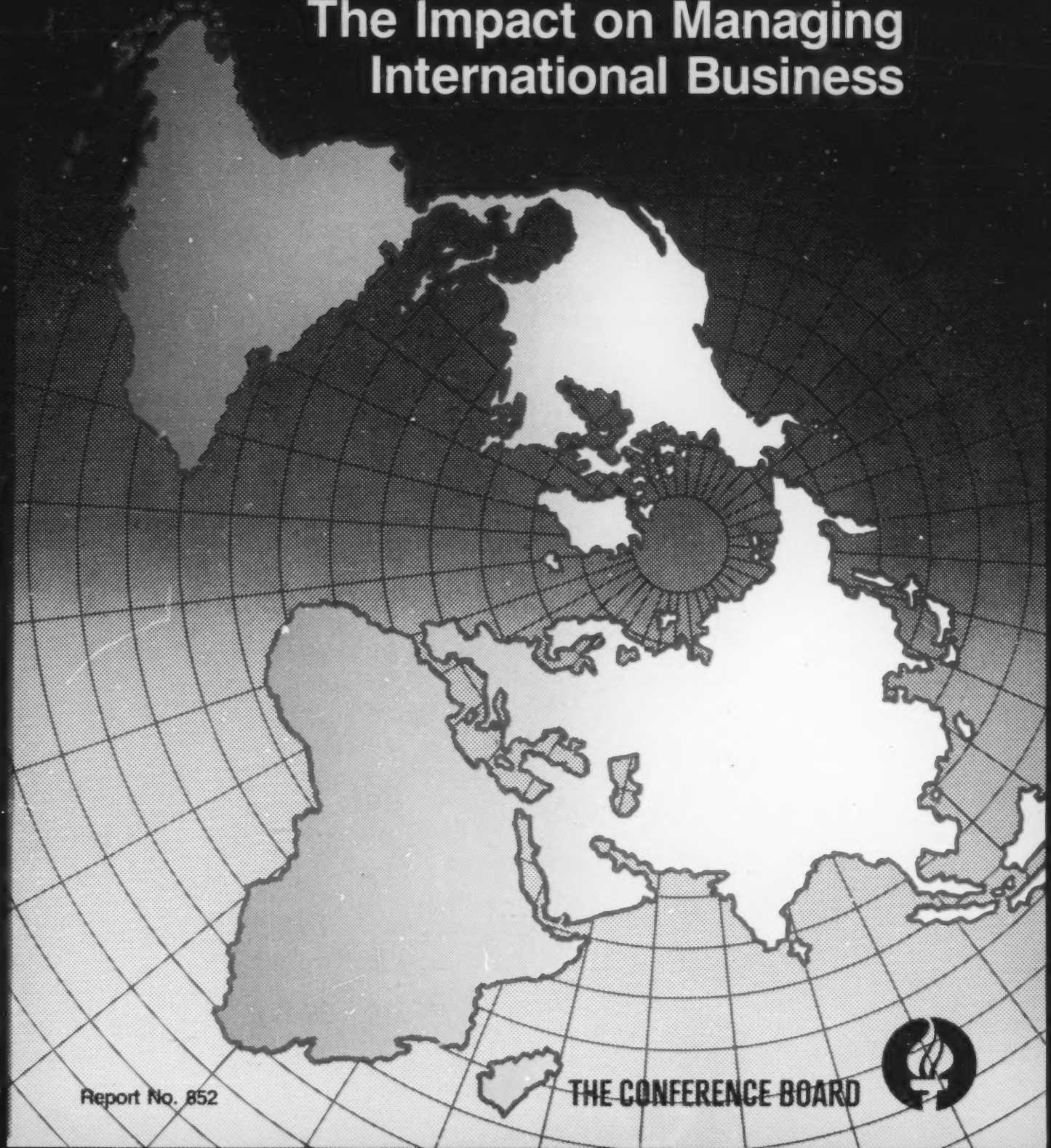
R4105-42

Regulating International Data Transmission: The Impact on Managing International Business



Report No. 852

THE CONFERENCE BOARD

ABOUT THE CONFERENCE BOARD

The Conference Board is a business information service whose purpose is to assist senior executives and other leaders in arriving at sound decisions. Since its founding in 1916, the Board has been creating close personal networks of leaders who exchange experience and judgment on significant issues in management practice, economics and public policy. The networks are supported by an international program of research and meetings which The Conference Board staff of more than 350 persons carries out from offices in New York, Ottawa and Brussels.

More than 3,600 organizations in over 50 nations participate in The Conference Board's work as Associates. The Board is a not-for-profit corporation and the greatest share of its financial support comes from business concerns, many with worldwide operations. The Board also has many Associates among labor unions, colleges and universities, government agencies, libraries and trade and professional associations.

The Conference Board, Inc.
845 Third Avenue
New York, New York 10022
(212) 759-0900
RCA International Telex
237282 and 234465

The Conference Board, Inc.
Avenue Louise, 207 - Bte 5
B-1050 Brussels, Belgium
(02) 640 62 40
Telex: 63635

The Conference Board, Inc.
1755 Massachusetts Avenue, N.W.
Suite 312
Washington, D.C. 20036
(202) 483-0580

The Conference Board of Canada
25 McArthur Road
Suite 100
Ottawa, Ontario, K1L-6R3
(613) 746-1261

Conference Board Report No. 852 Printed in U.S.A.

© 1984 THE CONFERENCE BOARD, INC.

ISBN NO.: 0-8237 0293-6

Cover by Virgil Koch.

Regulating International Data Transmission:

The Impact on Managing International Business

by James R. Basche, Jr.

A Research Report from The Conference Board

Contents

Page

WHY THIS REPORT v

I. ISSUES AND CONCERNS 1
Transmitting Data: A Corporate Management Concern 1
Transborder Data Flows 2
The Role of Technology 3
Service Industries 4

II. SURVEY RESULTS 6
Overview 6
A Cautionary View 7
Obstacles and Restrictions 7
Company Planning and Data Transmission Restrictions 10
Monitoring Developments in the Regulation of International Data Transmission 10
Changes in Ways of Doing International Business 11
Effects on Foreign Investment 13

III. INTERPRETING THE SURVEY RESULTS 14
Sources of Business Concern 14
Anticipated Growth of New Data Systems 14
Characteristics of Information 14
Broadening Restrictions 15
Governments' Concerns 15

IV. THE IMPACT ON MANAGING INTERNATIONAL BUSINESS 17

APPENDIX A 19

APPENDIX B 21

Why This Report

Financial, production, marketing, personnel, and R & D data exchanges among corporate units across national boundaries are growing as fast and comprehensive information becomes more critical to effective management. Any impediments to international data transmission may have seriously adverse effects on the competitive position of multinationals who rely on such information.

This study examines the kinds of regulations and obstacles governments are placing on data transmission, and the impact of such limitations on management. The study covers specific problems companies have already encountered and steps taken to meet those problems. It also may alert firms with plans to increase international data transmissions to developments that could hamper them.

The Conference Board is grateful to the 240 companies from 16 countries and to the more than a score of individuals who shared their experiences and knowledge in this area of growing concern to all companies conducting business in any way across international borders.

JAMES T. MILLS
President

I. Issues and Concerns

"The uncertainty surrounding the future availability and accessibility of communications networks has made planning for our long-term information needs on an international basis more difficult."

—E.I. DuPont de Nemours & Company

"In addition to the potential problems arising from data flow restrictions based on privacy considerations, we are also apprehensive about the regulation of data transmission networks, including restrictive technical requirements and tariffs, which is emerging in some countries and which could constitute further limitations on data network operations and planning. Another potential problem for us is the requirement in some countries that only nationally manufactured computer or telecommunications equipment or software can be used, inhibiting our selection of the most effective data processing and transmission alternatives."

—Mobil Oil Corporation

The two excerpts above were taken from letters sent in the Spring of 1980 to a U.S. congressional committee examining the field of international data transmission. At that time, corporate concerns for the management impact of government regulation of international data transmission seemed to be an issue of the future. For more than three-quarters of the companies (like the two quoted above) whose written replies were published in the congressional committee's hearings, international data-transmission restrictions presented more potential problems than real ones.[1]

However, a few companies reported that, by 1980, the growing number of government regulations that directly or indirectly affected international data transmissions had made some real impact on the management of their international business operations. Xerox, for example, reported to the committee that it had transferred processing of some payroll information from its own data center in London to a service bureau in Stockholm following the 1973 enactment of the Swedish data-protection law. Standard Oil of California wrote the committee that, to meet Canadian requirements, it kept a data-processing unit in Canada although its data-processing unit in the United States was capable of handling all its Canadian work. And CBS, Inc., reported that the U.S. State Department had blocked its use of the Intelsat satellite to send a news report on economic conditions in Cuba on the grounds that such news was not considered a "specific event of immediate international importance." Still, the examples described in the written replies and in testimony before the Subcommittee on Information and Individual Rights of the House Government Operations Committee came from a minority of companies responding to the congressional request for comments on corporate experience with the regulation of international data transmission.

In the next few years, various public and private groups were involved in a growing number of studies, meetings, speeches and publications on issues relating to international data transmission. The Conference Board decided to survey corporate experience anew to see what (if any) changes had occurred in international business operations as a result of new governmental policies, laws and regulations for this growing and important area of business activity.

Transmitting Data: A Corporate Management Concern

The basic corporate management concern with international data transmission does not change. Information or raw data are located in one place and are needed in another. Such information can be transmitted in several ways: It can be conveyed by voice on the telephone or in person; it can be hand carried; it can be sent by mail; it can be sent electronically by telex, by facsimile, by computer data links, by video, and soon by all of these seemingly at once using the technological miracle of ISDN (integrated services digital network). All of these electronic connections make use of telecommunications networks and some of them use computer links at one or both ends that may or may not process the data as well.

So long as the transmitted data are retained within the boundaries of one country the transmission can be

[1]U.S. House of Representatives, Committee on Government Operations. *International Data Flow.* Washington, D.C.: U.S. Government Printing Office, 1980.

Subjects Covered by the TBDF Label in Recent Literature

—Privacy and data-protection laws.
—Discriminatory taxation on imported computer and telecommunications equipment, software and information transfer.
—Costs of data transmission.
—Nontariff trade barriers.
—Building up local EDP and telecommunications-equipment manufacturing industries.
—Building up local data-processing and telecommunications-services industries.
—Technology transfer.
—National security restrictions on data transfer.
—National sovereignty and concern for information independence.
—Regulation of geophysical, natural resource, and map data acquired through airborne surveillance and remote sensing equipment.
—Equipment incompatibility (among nations).
—Restrictions on availability and use of leased lines.
—Assignment of radio frequencies.
—Use of geostationary (geosynchronous) orbit.
—Electronic mail.
—Restrictions and regulations of mailing lists used for international promotion and marketing.
—The New International Information Order.
—Restrictions on freedom of the press.
—International agreements covering freedom of information.
—Free trade in services.
—Copyright of software.
—Theft of copyrighted entertainment materials from international transmission services.
—Encryption and data security.
—Multiplicity of international (e.g., OECD, ITU, Council of Europe, UN) and national regulatory bodies.
—Political disputes (e.g., Arab-Israeli, West Africa, and South Africa) with consequences for international data transmission.
—Direct broadcasting services (DBS).

regulated, if desired, by the government of that country alone. Once these data cross international borders, however, they become subject to the regulations of all the countries concerned either acting independently under their own laws or jointly under international agreements. Corporate users of international communications facilities are subject to all such regulations, whether the facilities are owned by government (and most are government-owned monopolies) or by private companies. While no one country acting alone is able to force its laws and regulations governing international data transmission on other nations, this has not yet stopped any country from regulating its end of the international transmission line as it sees fit. Thus, companies are faced with a variety of national laws and interpretations of international agreements in their efforts to meet their basic management concern of transmitting information from where the data are located to where they are needed for their international operations.

Transborder Data Flows

Throughout this report, we generally refer to the subject as corporate management concerns with the regulation of international data transmission, rather than using the more common term of transborder data flows (TBDF or TDF). A perusal of the literature on this subject shows that the phrase "transborder data flows", like many other overused terms, has become increasingly meaningless. Paradoxically through use, TBDF has come to be used both too broadly and too narrowly.

Writings on and studies of transborder data flows are too broad in that they encompass much more than issues that are essentially "transborder" in nature. Many of the governmental concerns that have an impact on international data transmission are, fundamentally, internal national concerns such as the desire to build up local data-processing and telecommunications equipment manufacturing and service industries. A list of the wide range of subjects labeled TBDF in recent literature is given in the box above. The all-inclusiveness of the TBDF label dissipates the basic management concern of transmitting data from where it is located in one country to where it is needed in another.

In contrast to those who define TBDF too broadly, others (including a significant number of survey respondents) define the term too narrowly. They define TBDF entirely in terms of privacy and data-protection laws, overlooking other laws and regulations, especially economic and security policies, that affect corporate transmissions of data across borders. This narrow viewpoint is exemplified by a U.S. manufacturing executive: "We are sending only accounting, customer order, and invoice data across borders and, therefore, have not encountered any of the restrictions that might apply to personnel information."

This narrow focus, equating TBDF with privacy legislation, reflects several facts. The privacy of individuals was one of the first areas viewed as being threatened by the enlarged capacity for personal-data storage that came with computerization. More than a decade ago, this perceived

Countries That Have Existing or Are Considering Data-Protection Laws
(as of March, 1984)

Australia	Greece	Japan	Sweden
Austria	Gerrnan Federal Republic	Luxembourg	Switzerland
Belgium	(and several of its states)	Netherlands	United Kingdom
Canada	Hungary	Norway	United States of America
Denmark	Iceland	Poland	(and several of its states)
Finland	Ireland	Portugal	Yugoslavia
France	Italy	Spain	

threat led a number of countries, especially in Europe, to pass data-protection laws. These laws restricted the storage and the transmission abroad of certain kinds of personal information that had to be linked to specific individuals' names to be useful. For a list of the countries in which data-protection laws had been passed (or were being considered) as of early 1984, see the box above.

The national data-protection laws passed so far, or currently being considered, differ from country to country. Still, a number of provisions are common to most of them:

- Registration of name-linked data files is required. (Many of the laws refer to "automated" files, but a few countries require registration of manually kept files as well.)
- Information must be kept accurate and up-to-date.
- The purpose of the data file must be clearly defined and access to it must be limited to legitimate users for that specified purpose.
- Subjects of the data file have access rights to their files and the right to correct inaccurate data.
- Data authorities are established by the government to supervise compliance.
- Some laws require private companies to designate a data controller, who will be legally responsible for the company's compliance with the law.

The right of subjects to review the contents of their files has highlighted another, still unresolved, company concern about these privacy laws. The provisions of most of the laws apply to individuals. But a few countries—for example, Austria, Denmark and Norway—have extended these regulations to "legal" persons as well. Such an extension raises the question of whether companies in these countries will be allowed to find out what information about them is stored in the computers of their competitors.

As the number of national laws grew in Europe and elsewhere, the variations among them became increasingly apparent. Companies with operations in several countries were faced with different, and sometimes incompatible, data-protection requirements. The governments also recognized these problems, and efforts were begun to develop common standards for privacy protection on an international level. These efforts have resulted in a voluntary set of guidelines, approved and promoted by the Organization for Economic Cooperation and Development (OECD), and a Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, prepared by the Council of Europe to come into effect as a binding instrument when approved and ratified by at least five member states. As of March, 1984, three countries—Sweden, France and Norway—have ratified the convention and others are far enough along in the ratification process to believe the convention may become effective by the end of 1984 or early in 1985. (Excerpts from the OECD guidelines and the Council of Europe Convention are included in the appendices to this report.)

The widespread attention paid to the national data-protection laws and to the international guidelines and agreements by business organizations and the news media has led many business executives to view TBDF mainly, if not entirely, in terms of privacy protection. Because their companies do not transmit name-linked data across borders, they report that the regulation of international data transmission is a subject of little or no interest to them. In so doing, they are overlooking the growing number of restrictions affecting international data transmission that are based on national economic, security and cultural interests and are well beyond the privacy issue and its ties to specific name-linked data.

The Role of Technology

Much that has been written and said about the subject of international data transmission has been concerned with the dazzling technological achievements in data processing and in data transmission. The ever-enlarging capacities and ever-increasing speeds of these activities are wonders of the modern technical world that can easily mesmerize the nontechnical business manager faced with the problems of international data transmission. Yet, whether the means of transferring data are computer links in separate coun-

tries via satellite or the traditional postal system, the management task is basically the same: to get the data where they are needed. Limitations on use of postal, telephone and telegraph services (PTT's), can be as harmful to the firm's operations as limitations on the more dramatic new forms of transmission.

A manager can easily become fascinated by discussions of ISDN, satellites, fiber optics, modems and all the other technical aspects of data processing and transmission and lose sight of the basic management concern. With that in mind, The Conference Board decided to de-emphasize discussions of technical advances in this project and to ask the respondents about *any* kinds of obstacles they had encountered to the free transmission of data internationally—regardless of the means used.

While the decision is useful for this survey, technological changes cannot be completely overlooked; they play a significant part at some point in any discussion of international data transmission. The great advances in electronic data processing and storage, as well as in the speed of telecommunications, are the main reasons for renewed government attention and regulation in this area. If the technology for transmitting data had not changed, governments would probably not have sought new regulations.

Of even more importance for any study of this subject is the tremendous lag between technological advances and social action. Data processing and transmission are continually bounding ahead; governments tend to move very slowly. The gap between the speed of technical changes and the continuing slowness of governmental processes is widening. Some business and government leaders recognize that regulations drafted in the 1970's—but still not passed—have little relevance to the technology of data processing and transmission in the 1980's. One European business executive pointed out that some government regulations talk of "main frames" at a time of rapidly spreading use of minicomputers; and they refer to "massive data archives" at a time of distributed information rapidly assembled through telecommunications when needed. A U.S. executive in the survey concluded: "I believe that the demands of the marketplace and the surge in capabilities (satellites, etc.) will make most attempts at regulation by slow-moving governmental organizations ineffective."

Another area in which technology at least indirectly affects the regulation of international data transmission is in the growing capacity for data processing, storage and transmission beyond the immediate needs of many, if not most, users. Several European respondents raised this point. A German executive, for example, wrote: "From time to time we have the feeling that we could save some money by discontinuing the preparation and transmission of data not really needed by anybody."

Another executive, who is a data-processing and transmission expert as well as an authority on management-information systems for a major Dutch multinational company, emphatically affirmed this view. He commented that much of the data collected for a particular decision by a business manager is unique to that decision and, therefore, will not be used again and need not be stored. He estimated that, currently stored in computers, billions of bits of data will never be used by any manager to improve decision making. Corporate headquarters often request data from their foreign subsidiaries for which they have no real use. Part of this collection, storage, processing and transmitting of data not used by anyone can be traced to users' fascination with large capacity processing and transmission equipment. People say: "The capacity is there, let's use it." This, he believes, is an irresponsible use of what should be a management tool and can unnecessarily arouse the suspicions of government officials wary of private companies—especially foreign private companies—that store vast amounts of data about their economies and their citizens.

Service Industries

Service industries—including those that provide data-processing and transmission services, banking and other financial services, insurance, shipping and the travel-related industries have long led the private business sector's discussions of government restrictions that might be placed on the international transmission of data. This is to be expected; the essence of much of their business is the transfer of information, often across international borders, much of it name-linked.

At the beginning of 1984, for example, SWIFT (the Society for Worldwide Interbank Financial Telecommunication) was handling about 500,000 transactions a day over its special communications network among its 1,200 bank members in 52 countries, and its services are steadily growing. During 1982, SITA (Societe Internationale de Telecommunications Aeronautiques), a network of leased lines to handle reservations among 243 airlines, sent more than 5.7 billion messages over its network.

A single U.S. service company, American Express, spends $300 to $400 million a year to operate its worldwide data-processing systems and communications networks. Besides reporting that figure, in April, 1983, at a European seminar, a senior vice president of American Express described the extent of some of his company's data-communications and processing operations.[2] They included processing 350 million credit-card transactions annually; handling $10 billion a day in international banking transactions; processing 56 million insurance premiums and claim transactions annually; handling communications on

[2]Harry L. Freeman, "A User's View of International Communications." A speech delivered at a seminar on Communication, Regulation and International Business, sponsored by the International Management Institute, Geneva, Switzerland, April 13, 1983.

the sale, verification or replacement of travelers checks sold by more than 100,000 banks and other outlets around the world; and handling 500,000 daily messages concerning other financial transactions. For companies in these service activities, a very large proportion of these messages and transactions must be specifically linked with individuals' names.

SWIFT, SITA, American Express, and a few other organizations (mainly services) have spent much time and money keeping themselves informed about national and international regulation of data transmission. A review of the recent literature in this field shows that executives of these groups have often been willing to share their experience with other companies and business organizations.

Many other companies with international markets and operations, especially manufacturing and other nonservices companies, have had much less experience in this area and have, consequently, paid less attention up to now to the potential limitations on international data transmission. The principal manufacturing exceptions, again as could be expected, are the manufacturers of equipment for the data-processing and telecommunications industries.

Because the concerns of the international service companies, expressed through publications and in testimony before government bodies, are better known, The Conference Board decided to concentrate this survey on the lesser-known experiences and concerns of manufacturing, mining and other nonservices companies. More than 90 percent of the requests for information were sent to nonservices companies in manufacturing and mining, and 91 percent of the usable replies were from companies in this category. (See box.)

Manufacturing and other nonservice companies that do not currently have any major primary concern with restrictions on data transmission across national borders may still have an important secondary concern. If a company does any international business at all (ranging from exporting to the operation of large-scale manufacturing facilities in other countries) in today's business world, it must make use of companies that provide international business services. Any restrictions on the latter's transmission of data can have an adverse effect on the business of the former.

Distribution of Survey Replies

Geographic Distribution

Area	Number of Letters Sent	Number of Usable Replies	Percent of Usable Replies
Canada	96	30	31
Europe	205	64	31
Japan	13	1	8
U.S.	768	145	19
Total	1,082	240	22

Industry Distribution

Area	Manufacturing and Other Nonservice Companies	Service Companies	Business Organizations	Total
Canada	26	4	0	30
Europe	54	9	1	64
Japan	1	0	0	1
United States	138	7	0	145
Total	219	20	1	240
Percent of total	91%	8%	<1%	100%

This possible secondary effect was clearly recognized in the survey response from a major British industrial firm: "Our operations are considerably affected by the convenience and efficiency of service-sector industries like banking, insurance, shipping, air travel, specialized information services, and so on. They depend heavily on international data transmission." In this sense, all companies with international business have some real concern with the political, legal or technical developments that might restrict the international transmission of data whether the effects are immediate and direct or delayed and roundabout.

II. Survey Results

During the Summer of 1983, The Conference Board sent survey letters to 1,082 companies in 20 countries. The letters contained four sets of questions covering corporate experiences with: (1) all obstacles or restrictions to the transmission, by any means, of internal company data across international borders; (2) any changes in the ways companies conduct international business as a result of those barriers; (3) any increases in costs of doing international business as a result of those barriers; and (4) any consequent effects on their foreign investment decisions. The questions were open-ended and allowed the respondents to reply at the length they felt appropriate and to add any other comments they believed to be useful.

Usable replies were received by the end of 1983 from 240 executives (22 percent) representing 239 companies and one business organization. The usable replies came from companies in 16 countries: Austria, Belgium, Canada, Denmark, Finland, France, the German Federal Republic, Greece, Ireland, Japan, the Netherlands, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

The written responses were supplemented by interviews and discussions with 24 respondents and other persons knowledgeable in this area of business activity in Belgium, Finland, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States.

Because of the decision to emphasize nonservice company users, most of the responses were from manufacturing companies drawn from a variety of industries including chemicals, pharmaceuticals, machine tools, mining, petroleum, construction equipment, iron and steel products, textiles, EDP and telecommunications equipment. The small number of service companies included banks, insurance, other financial services, shipping, EDP and telecommunications services, publishing, retail stores, and construction.

Throughout this survey report the single reply from a Japanese company is included in overall totals where it responded, but no effort is made to discuss it separately.

Overview

National and international restrictions on the transmission of internal company data across international borders are still a problem for the future—if considered at all—for a large majority of the companies responding to The Conference Board's survey. Of 238 companies answering a question about their corporate experiences in this matter to date, 181 (or 76 percent) reported that they have not encountered any obstacles or restrictions to the international transmission of internal data. Although the proportion of services companies encountering such barriers was higher than the overall response, even among that small group 58 percent said they had encountered no such obstacles.

Among a group of 57 respondents who made specific comments about their expectations, uneasiness about possible future restrictions on international data transmission was more apparent. Forty-nine (86 percent) respondents reported serious concern that any future data-transmission regulation by governments could have an adverse effect on their international business operations.

Answers to the three other major survey questions support the general view that regulatory restrictions on international data transmission is not currently a major concern among most industrial users:

- Of 189 respondents, 88 percent said they had made no changes in the way they do international business as a result of any limitations on international data transmission.
- Of 191 respondents, 87 percent said they had experienced no increase in the costs of international business attributable to restrictions on international data transmission.
- Of 188 respondents (including many reporting that they had already encountered some obstacles), 99.5 percent said restrictions on international data transmission had not yet had any effects on their foreign investment decisions.

In the late Fall of 1983, the OECD published the results of a survey of corporate experience in this area. The number of firms in that survey was somewhat fewer than the number in this Conference Board survey. Still, the general conclusion of the OECD survey was much the same: "Overall, the impression left by the responses to this

Countries and Regions Named Where Obstacles Were Encountered

Area	Number of Times Cited	Area	Number of Times Cited
Argentina	1	Mexico	7
Australia	1	Netherlands	2
Austria	6	Pakistan	1
Brazil	20	Philippines	3
Canada	12	Poland	1
Chile	1	Scandinavia	1
Egypt	2	Singapore	1
Europe	7	South Africa	5
France	2	South Korea	2
German Federal Republic	11	Spain	1
Hong Kong	1	Sweden	1
India	2	Switzerland	1
Indonesia	1	Taiwan	3
Ireland	2	United Kingdom	5
Japan	1	United States	3
Latin America	4	Venezuela	1
Malaysia	1	West Africa	1

survey is that while there are not serious problems at present, the issues have not been finally resolved and, at least in the banking sector, some concern is apparent below the surface."[1]

A Cautionary View

Although there is apparently limited concern with this issue among manufacturing concerns with international business, respondents caution against exaggerating the problem. A Dutch executive of a major multinational manufacturing firm said (in a telex reply): "As a general remark we would like to say, that, of course, the problem should not be ignored; however, we have the impression that it gets too much attention and therefore tends to become exaggerated." The significance of this reservation was underlined in a later interview with executives of this company, in which they indicated the thought and experience that had gone into their cautious statement. Their firm is one of the few in this survey to have had an internal group formally monitoring developments for several years in government regulation of international data transmission in countries in which they have operations. Their reservation about the possible exaggeration of the TBDF issue is based in considerable part on the experiences of this monitoring group. (See below, page 11.)

An executive of a large German firm expressed a similar reservation: "A lot of fears and concerns have been expressed which, in our view, are based on feelings of uneasiness rather than on facts." While this, like most similar comments in letters and interviews, came from European executives, they were not exclusively reservations of the Europeans. The head of corporate communications for a major U.S. electronics firm, for example, wrote with regard to U.S. company fears of the results of European data-protection laws: "I think the privacy problem is more imagined than real."

Obstacles and Restrictions

A large number (although still a minority) of all the respondents report already having encountered some sufficiently serious obstacles or restrictions on international data transmissions for their companies to view the issues with real concern. Of 238 companies answering the survey question about obstacles or restrictions *already* encountered, 57 (roughly one in four) reported having had such experiences. They reported these encounters in 30 countries. The full list of countries and regions named and the number of times each was cited is shown in the box above. Leading the list in frequency of citations are Brazil, Canada and the German Federal Republic.

European-based companies proportionately reported encountering obstacles or restrictions in international data transmission more often than others. Eighteen European companies (29 percent of those replying) said they had encountered some types of obstacles or restriction in this area of business concern. Of the responding U.S. companies, 25 percent reported obstacles, and of the Canadian group only 10 percent reported any difficulties.

[1]Organisation for Economic Co-operation and Development, Directorate for Science, Technology and Industry, *Transborder Data Flows in International Enterprises: Based on Results of a Joint BIAC/OECD Survey and Interviews with Firms.* Paris: October 1983, p. 35.

Kinds of Obstacles and Restrictions Encountered

Legal Regulations

—Privacy and data-protection laws.
—Requirements to use locally manufactured EDP and telecommunications equipment and software.
—Requirements to process certain kinds of data locally.
—Requirements to maintain certain business records within a country—sometimes making it necessary to duplicate them.
—Requirement to send data abroad through a single border gateway.
—Prohibition on connections between leased lines and public telephone networks.
—Prohibitions of on-line connections for sending order and shipping information.
—Prohibition on the use of dial-up data transmission.
—Restrictions on intercompany exchange of exploratory data involving natural resources.
—Restrictions on technology transfer and export licenses for diskettes containing specified company information.
—Restrictions on using word-processing equipment for communications.
—Restrictions on using electronic mail systems.

PTT Regulations and Practices

—Refusal by some countries to accept certain kinds of mail, including diskettes and tapes.
—Restrictions and delays in making leased lines available to private companies.
—Tampering with mail containing tapes and diskettes.
—Tapes put through X-ray machines, thus corrupting the data.
—Martial-law restrictions on telex and mail.
—Monitoring by governments of data sent through PTT facilities.
—Customs delay on diskettes sent through the mail facilities of PTT's.

Technical

—Incompatible equipment standards among countries.
—Delays caused by lack of adequate facilities.
—Garbled or slow transmission of data due to poor quality of equipment.

Miscellaneous

—Political restrictions on data transmission to proscribed areas
—Linking government approval of unrelated business plans to company EDP and telecommunications policies and practices.
—Threats that governments may tax data transmission.
—Prohibitive costs, including high tariffs on leased lines, data-transmission services, EDP and communications equipment.
—Strikes, slowdowns and other labor difficulties at PTT and other transmission facilities.

As was to be expected, service companies also reported proportionately more difficulties than did manufacturing firms. Although the service companies comprised only 8 percent of the total respondents, they make up 14 percent of the number reporting difficulties in the international transmission of internal company data.

The survey asked companies to report any relevant obstacles encountered and did not limit the kinds of difficulties reported to those directly related to electronic transmission of data. Thus, the reported obstacles covered a range that included some situations that would ordinarily not be reported in the TBDF studies that emphasize computer processing and advanced electronic-transmission systems. Among the obstacles reported that might not usually be considered in TBDF studies are labor difficulties at transmission facilities, customs delays with data sent through the mails, and the corruption of data on tapes exposed to some post-office X-ray machines. This difference gains added significance because, even including this broad group of obstacles, fewer than one-quarter of the total respondents indicated that they had encountered any limitations on their transmission of internal company data across borders. This underscores the overall view that, for the majority of users—especially manufacturing firms—this is an area for future concern, if any, rather than current concern. It adds some support to the general reservation of a number of respondents that this problem may currently be exaggerated. Several companies described the obstacles they have encountered. All reported obstacles are listed in the above box.

Privacy and data-protection laws, especially as applied to customer data, personnel data, and registration of data bases, were the most frequently cited restrictions on international data transmission. Local legal requirements for data protection often are met by setting up independent data-storage and processing facilities for each country. Several companies pointed out, however, that the data-protection laws were only one of several reasons for setting up such local facilities. Other business reasons such as costs and plans for future development, were often cited as playing a more important role in the decision to set up local EDP operations.

Other obstacles frequently cited by the respondents were the poor quality of transmission equipment in many parts

of the world, especially in the developing countries; the high costs of data transmission in some developed and developing nations; and the requirement by several countries that companies use locally produced EDP and telecommunications equipment.

Brazil, the country most often named by respondents as the one in which obstacles were encountered, achieved its first place largely due to its requirement that companies use locally made equipment and software. This requirement reflects a Brazilian economic (rather than a privacy) policy that has become gradually more restrictive over the last decade. In a report submitted to the United Nations Centre on Transnational Corporations by the Brazilian government and published by the United Nations in 1983, Brazil clearly explains the economic reasons for its restrictive informatics policy and sets forth these objectives:[2]

"To obtain the technological capacity that would enable electronic equipment and software to be designed, developed and produced in Brazil;

"To ensure that national corporations play a predominant role in the national informatics market;

"To obtain a favorable balance of payments in products and services related to informatics;

"To create jobs for Brazilians and more professional employment opportunities for Brazilian engineers and technicians; and

"To create the opportunity for the development of a Brazilian parts-and-components industry in informatics."[3]

The practical effects of this Brazilian policy is to limit the kinds of EDP equipment multinational companies can use in that country. A Finnish company reported that the Brazilian equipment requirement resulted in the firm's use of locally produced equipment, which is incompatible with its worldwide EDP system, for its internal budgeting and controlling. Instead of receiving budget reports from its Brazilian affiliate through its worldwide EDP system, Brazilian reports are received through standard telex transmissions. Brazil has taken the world lead in restrictions on the kinds of equipment that can be used for EDP and telecommunications. For this reason, its experiences are considered worth watching for any ripple effects on other developing countries.

Brazil, however, was not the only country reported as having equipment limitations for international data transmission. One European company reported the government of Ireland's requirement that only the modems provided by its post office be used. The company said the modems were satisfactory, but more expensive than those available from other suppliers. A Canadian company felt its data transmission choices were limited by its own government's demand that a Canadian satellite be used for any data transmissions.

Canada's position as the second most frequently cited country, after Brazil, does not rest so heavily on one particular type of restriction; responding companies reported several different kinds of restrictions in Canada. The satellite-use limitation was one. Restriction on the number of gateways for international data transmission from each province was another that was cited several times. A U.S. manufacturing executive indicated that this rule permits the Canadian government to dictate the routing of data transmissions, which can raise costs. Both manufacturing and service companies reported another obstacle to international data flow: the Canadian requirement that certain kinds of data must be processed and stored in Canada. This sometimes results in unnecessary duplication of services and facilities.

To get a Canadian charter an international financial-services company, based in the United States, was required to do all data processing for its Canadian operations in Canada. In another instance involving a services company, Canada linked together two otherwise unrelated regulations—approval of an acquisition and data processing: "In order to gain approval from Canada's Foreign Investment Review Board for a planned acquisition, we agreed to repatriate data-processing activities for our other Canadian business operations. This business has been supported from a U.S. data center via telecommunications for the past twelve years."

West Germany is the country cited third most frequently for the obstacles it generates. The restriction most often reported, in addition to its privacy legislation, was the German regulation prohibiting the connection of the public telephone network and private leased lines.

Another area of concern reported by several companies is the desire of some governments to protect national-security interests by monitoring all international data transmissions. Two manufacturing companies specifically mentioned the Taiwan government's attempts to carry on such monitoring activities. One of these firms reported delays in Taiwanese customs offices of shipments, including diskettes, so that the government could try to read them. Still another firm reported problems of this kind in a different geographic region. Under a law (since revoked) of an unnamed Middle Eastern country, the company had at one time been required to reduce the speed of its international data transmission so that it would be feasible for the local government, using less sophisticated equipment, to read the firm's transmissions.

[2]Special Secretariat of Informatics of the National Security Council of the Presidency of the Republic of Brazil, *Transborder Data Flows and Brazil: Brazilian Case Study*. United Nations, New York: UN Centre on Transnational Corporations, 1983, p. 64.

[3]"Informatics" is the field of activity dealing with the automatic processing, storage and distribution of data. The term has been adopted officially by several governments and government agencies — for example, a Special Secretariat for Informatics in Brazil and the Intergovernmental Bureau for Informatics set up by the United Nations.

Among more than three-quarters of the respondents who reported that their companies have not yet encountered any obstacles or restrictions, several volunteered explanations. The one most often given was that the organizational structure of the companies had forestalled any government-imposed limitations. Foreign subsidiaries were described as autonomous units, with their own data-processing and storage facilities. These firms pointed out that very little data had to be sent across borders, that the data were usually aggregated, and did not ordinarily include name-linked data that might contravene privacy-protection laws. Several emphasized that the decision to make subsidiaries independent was made for various management reasons and that the data-transmission issue was only one of many considerations. But this management decision had the positive effect of helping the companies make their data-transmission operations conform to the laws of the various countries in which they worked.

A second explanation given for the apparent lack of obstacles was the current lack of electronic links among many corporate units. This referred to the lack of company EDP and telecommunications links rather than to the older telex and telephone connections. A number of these reporting companies, however, are moving toward the installation of newer telecommunications and EDP links. They are among the firms that expressed concern about the future effects on their businesses of existing and proposed government regulations. Concern was also expressed by a few companies that foresee the possibility that future government regulations will not apply solely to electronically processed data. The data-protection laws in a few countries (e.g., Greece) already propose to apply restrictions to manually processed, as well as electronically processed, files.

Company Planning and Data-Transmission Restrictions

Despite the present limited concern about data-transmission restrictions, a number of companies reported they are sufficiently concerned about the future impact of such restrictions on their international business operations to consider the issue in their current planning activities. Sixty-seven respondents commented on the effects of this issue on current planning. Of this number, 23 (or slightly more than one-third) said they did consider existing or potential data-transmission restrictions in planning their future international business development.

The concerned companies included some that had already encountered obstacles and others that had not. Among the former was a U.S. manufacturer of environment-control equipment: "This area is of some concern to us because of a variety of plans we are currently formulating to implement additional telecommunications capabilities on a worldwide basis. There is no doubt that those legal, technical and practical obstacles or restrictions to cross-border data transmissions that do exist will exert significant impact on our decision-making process in the future."

A U.S. chemical company that has not yet encountered any restrictions is still concerned enough about the possibility to incorporate specific study of this issue into its planning process: "We have been giving serious consideration to electronic computer links using value added networks and dial-up telephone links directly between headquarters and the overseas location. As a result, we have been investigating the potential problems affecting this data transmission and it definitely has an impact on our planning."

These responses, typical of those from firms commenting on data transmission regulations and their impact on corporate planning, have one thing in common: As could be expected, the most concerned companies are the ones with plans to initiate or to expand existing data transmission systems to aid their international business operations.

Monitoring Developments in the Regulation of International Data Transmission

As part of their planning activities or of their general concern about the impact of data transmission on international business operations, a number of respondents indicated that their companies regularly monitor developments in the areas of national and international regulations on data transmission. For many of these companies, this monitoring consists mainly of keeping up with the current periodical literature and specialized reports on the subject. Others supplement that internal monitoring by participating in the monitoring activities of their industry associations and of concerned international business organizations. Among the international business organizations cited as following the issue were the International Chamber of Commerce (ICC), the Business and Industry Advisory Committee to the Organization for Economic Cooperation and Development (BIAC/OECD), and the International Telecommunications Users Group (INTUG).

The ICC and the BIAC/OECD groups have made studies of various aspects of business concerns on this issue and have represented the international business community before government agencies and international organizations that undertake regulation of international data transmission. Both groups are broadly based geographically and in their constituencies. In contrast, INTUG, as indicated by its name, is mainly representative of the segment of the business community that uses international telecommunications facilities. A relatively new organization of national user groups, with a few large companies having associate status, INTUG presently is active in only a few countries, but is growing.

A Finnish executive, whose company is associated with INTUG, described its value to his firm. The organization keeps his firm informed, often in advance, of changes in national PTT regulations and how they will affect users.

Through INTUG, his company can make contacts with other multinational companies and national user groups to discuss local user problems in those countries where the firm operates. As an associated company, the Finnish firm receives publications from user groups in other countries. These publications enable the firm's staff to become familiar with telecommunications problems and with telecommunications-equipment vendors in those other countries. They find the organization is also useful for exchanging information on new products and other technological developments in the telecommunications field. Both Finnish and British executives mentioned that INTUG represents users' viewpoints before equipment and facilities standardization committees of the International Telecommunications Union (ITU), an official intergovernmental organization regulating this field, and it cooperates with the ICC and BIAC/OECD in representing business' viewpoint before other government bodies.

In addition to monitoring the relevant literature and participating in concerned international business organizations, two respondents mentioned their companies' plans and efforts to set up formal task forces to monitor developments in this area. An executive of a U.S. conglomerate wrote: "We are in final stages of completing a formal, long-range technology strategy for our company of which telecommunications is a major section. Within that section, we address the issue of transborder data flow with a current assessment of our understanding of the situation in various countries in which we have significant business ventures; and a recommendation to form a permanent task force composed of information services, legal, audit, security, and business-unit personnel to pursue vigorously the future impact that governmental policies will have on our ability to conduct business in various countries."

While the U.S. company's monitoring task force was still in the planning stage, a Dutch manufacturing company reported having established such a task force several years earlier. It was set up when the West German government passed a law requiring each company to have a data-security officer who would be personally responsible for that company's compliance with the German data-protection law. The Dutch company complied with the specific law but also felt the time had come to pay more attention to this whole developing issue on a worldwide basis.

An internal committee was set up at corporate headquarters in the Netherlands to monitor this issue in all countries where the company operates. The committee was made up of representatives from several headquarters staff groups, including accounting, legal, communications, EDP, and a separate group called "message delivery service." The committee holds eight to ten short meetings a year to discuss items brought to its attention from any of the company's operations around the world. Members of the committee also represent the company on this matter in the Dutch employers' organization and in appropriate committees of the ICC.

After several years of this work, however, the company is beginning to play down the whole issue. Committee meetings have tended to decrease in number and in length. Their monitoring experience has led them to feel that the only companies seriously affected by the laws so far passed are relevant equipment manufacturers, EDP and communication-service providers, and a few large service company users of international data transmission facilities. The company plans to continue monitoring activities, probably on a less formal basis, as a kind of advance warning system, but it expects to be spending less effort on this issue in the future.

Changes in Ways of Doing International Business

Few of the companies who participated in this survey have changed their ways of doing international business in response to government restrictions on international data transmission. Of the total respondents, 189 firms answered the question on the effects of data-transmission limitations on their way of conducting their international business operations. Only 23 (or 12 percent) reported making any changes attributable to this factor.

The most common change reported is the reorganization of the company's EDP from a central corporate function to one that is geographically distributed to reflect national policies and restrictions on the transmission of data across borders. With regard to the effects of the German data-protection law, for example, the president of a Dutch company explained: "This law prohibits the transfer of data with respect to personnel across borders, unless guarantees are provided that these data are kept confidential. As this confidentiality could not always be guaranteed, we had to reorganize the computer programming and operations with respect to personnel data in such a way that they are no longer handled centrally at our data center in Holland but separately in Germany."

A U.S. company reported: "Our data-processing strategy eliminates the need for international data flow as we have established independent data-processing facilities and record-keeping operations within each country. This data-processing strategy is based upon the assumption that multinational sharing of data-processing centers will ultimately be unfavorably affected by transborder data flow restrictions."

Other companies on both sides of the Atlantic reported that restrictions on EDP links across borders led them to use other methods of transmitting data between countries. Several use couriers to deliver tapes and diskettes to countries in which they have had postal and customs delays involving those items as well as to countries without EDP connections. One company has shifted to using regular telex transmissions to report data from those countries

where it has not been able to set up EDP connections because of government restrictions.

Some companies reported that they simply limit the kind of data they send across borders in order to avoid certain government restrictions; some firms send no payroll or other personnel data; others process all their orders locally. One petroleum company reported that it made certain not to transmit any data at all through countries where it does not have operations. A German company uses the computers of a joint-venture partner in Brazil and does not link its operations there to its worldwide data network. One European company said it keeps a duplicate set of books for its Philippine operations outside that country.

Significantly, no company reported making any major organizational changes as a result of limitations on its capability to transmit data across borders. The changes reported were functional ones, mainly confined to the EDP function.

Cost Increases Due to Data-Transmission Restrictions

Among 191 companies responding to a question about cost increases in their international operations due to limitations on transmitting data, 25 reported increased costs as a consequence. Among the small number of service companies, the proportion was higher, slightly more than one-quarter reported higher costs of doing business abroad due to data-transmission obstacles and restrictions.

While most of the firms reporting increased costs attributable to data-transmission restrictions were able to point to factors they believed to be responsible for such increases, only three companies were able to estimate actual cost increases. For these three companies, the annual increases reported ranged from $40,000 to a possible $200,000. For these three and other companies, the cost increases were attributed to:

- The need to set up separate EDP systems in some or all countries where individual firms operate so as to meet local laws and regulations.
- The need to duplicate data bases and other systems in several locations. (A U.S. firm, one of the three reporting actual cost-increase figures, said duplicating ledger systems in Canada and the United States to meet Canadian requirements were raising its costs of doing business in Canada by between $150,000 and $200,000 a year.)
- Technical restrictions. (For example, the Canadian requirement that Canadian companies use Canadian satellites; Ireland's requirement that companies operating in that country use only the official post-office modems; and German restrictions on the interconnection between public telephone networks and private leased lines. One U.S. company estimated that this last restriction had raised its costs by $100,000 to $200,000.)
- The need to switch to alternative means for data transmission (e.g., a switch from EDP transmission to telex or courier services) and for data processing. An example of the latter is provided by a U.S. bank that has had to use outside service bureaus instead of its central worldwide EDP services for certain accounting and other banking operations in order to meet government restrictions on the transmission of such data in several European countries.
- The need to set up special administrative procedures to meet requirements of various European data-protection laws was reported by U.S., Austrian and Danish companies.
- The inability of a company to choose the most direct routing for its data transmissions due to government restrictions (reported especially by Canadian companies).
- The need to monitor developments in international data transmission.
- The many restrictions in Brazil that cause data-transmission delays and require the use of special equipment. (A British company reported extra costs of about $40,000 a year to install excess capacity in order to overcome the difficulties of upgrading processors in Brazil.)

In addition to these cost-raising factors, one U.S. company foresees a possible future problem that is already a real problem for a European company. The U.S. executive wrote: "Our widespread use of electronic mail between locations in the United States, Europe and Japan reduces revenues of the postal authorities of those countries. One day they may try to find some way of compensating for the lost revenues."

A European telecommunications-services company has already encountered government agencies seeking compensation for lost revenues. The company operates a large-scale private communications network providing services to other firms. Because most of the transmission facilities in Europe are owned by the government PTT monopolies, the firm must lease lines from several of these government-owned companies. Some of the government-owned companies are charging the private network fees three to ten times above their ordinary rates and are justifying these high charges, at least in part, as compensation for lost revenues to the PTT's own telecommunications operations.

A different worry about the future was expressed by a U.S. company that manufactures EDP equipment. At the present time, it has no increased costs attributed to limitations on data transmission, but it sees this as a real possibility if and when the Council of Europe's convention on data protection becomes law. The firm believes that the requirements of the convention could increase the costs of EDP and telecommunications systems for all users in countries adhering to the agreement.

One U.S. company reported that data-transmission limitations had not yet increased its costs of doing business abroad. However, the company was disappointed in such

limitations, and felt they had had a negative impact on its operation. This company had expected to reduce its costs by maintaining central payroll operations. Data-protection laws in individual countries had prevented the firm from doing so, thus eliminating its anticipated cost savings on that portion of its international operations.

Effects on Foreign Investment

Despite experiences with regulations and costs, government limitations on international data transmission have not yet affected the foreign-investment decisions for the overwhelming majority of responding firms. Only one of 188 companies replying to this question reported any specific instance of changing or modifying an investment decision because of restrictions on data transmission. A U.S. electronic-equipment manufacturer reported making a decision to place an overseas manufacturing facility in one country rather than another on the basis of many factors, "of which TBDF was one."

However, other companies mentioned giving some general consideration to this issue or the possibility of future consideration. A U.S. textile company reported: "We must consider adverse action by national authorities affecting transborder data flows, among other issues, in dealing with potential investment decisions for activity outside the United States." And a U.S. food products executive said: "Stringent regulations on data transmission would certainly be a strong factor when we consider starting operations in new countries."

A Swedish business leader concisely summed up the concerns of many companies about the possible future impact on their investment decisions: "It is clear that the national climate for computers, TDF, and so on, is becoming one important issue when deciding where to locate operations. Severe difficulties in operating computerized networks between countries, as well as in importing and attaching the most appropriate equipment, will influence the location of major installations in the form of company data bases, design centers, supply centers, and so on. Central company functions cannot be placed in countries with very complicated and odd TDF legislation, PTT conditions, and the like."

III. Interpreting the Survey Results

In view of the limited encounters with government obstacles to international data transmission reported by the survey participants and the even more limited effects of such encounters felt by many of them, the question to be asked is this: Why does an uneasy concern about these issues persist in the private international business community? Answers can be found in the general comments of the respondents to The Conference Board's survey, in the interviews, and in recent literature on the subject.

Sources of Business Concern

First, enough examples of government efforts to restrict the transmission of data across international borders have already been reported and are well-known within the business community to alert international executives to the realities of these issues. Even if the restrictions have not had an effect on their particular companies or industries, there is no reason to assume they might not have an impact in the future. Some of the obstacles reported may be due largely to incompetence or to meddlesome government workers in PTT's and customs offices seeking to exert their authority. But not all limitations, as a growing number of international companies are coming to realize, can be blamed on bureaucratic bumbling. Private companies are beginning to realize that some restrictions—such as the absolute prohibition on transmitting certain kinds of data or the requirement that data generated within a country must be processed and stored there—are the result of formal, long-range government information policies.

Anticipated Growth of New Data Systems

Executives are also well aware that electronic data processing and information communications are rapidly growing in importance for all businesses. They are especially useful for multinational businesses for which distance and time differences are significant factors in operations.

As the number and efficiencies of EDP and telecommunications systems grow, competitive needs will compel more and more companies to use these advanced systems in more and more operations, including their international operations. As these systems become an essential, rather than a merely useful, part of international business operations, any restriction on their use will become a matter of major concern to multinational companies. This point was made clear by a U.S. pharmaceutical executive: "We are becoming increasingly committed to the electronic transmission of data across country borders, primarily through the use of word-processing equipment tied in with computers, and this gives rise to a concern about the impact of laws and regulations that seek to limit or restrict the transmission of internal company data across borders."

Characteristics of Information

Certain characteristics of information transmitted internationally also contribute to the uneasiness felt by company executives on this subject. Information sent across borders can be divided into two main groups: internal company data (such as personnel records, production and financial data) and data obtained (usually purchased) from sources outside the company—mainly from data bases and archives of different sorts. The latter data include mailing lists for direct marketing campaigns, scientific and technical papers used for research, and economic statistics about a country or an industry in which a firm is interested. The Conference Board's survey was concerned mainly with internal data exchange, but some respondents expressed more concern about purchased data. In these instances, the data become a kind of commodity.

As a traded commodity, information differs from other products. Most products in international trade are sold, used and consumed. Information can be sold and used, but it is not usually consumed. It can be resold and reused repeatedly, and may even become more valuable with reuse. This unique quality of information as a commodity and the differences between information purchased from the outside and internal company data raise questions not yet fully answered to the satisfaction of most international business executives. Should laws that restrict the international transmission of personal information (salary levels, home values, personal hobbies) sold for use in direct-mail marketing campaigns, for example, also be applied to the international transmission of the same information for use entirely within a company for the evaluation of an employee being considered for promotion?

If information is treated like other internationally traded commodities, how will its value be assessed for tax purposes—as is being suggested by some government officials? Will information sent between a corporate headquarters and a foreign branch be assessed at the same value as the identical information sent to a licensee for a fee or sold outright to a foreign firm? If information is treated as an international commodity, will it be subject to other commodity regulations such as a requirement to ship a certain proportion by national carriers? (Canadian executives in this survey reported their government's already-existing requirement that its satellite be used by Canadian-based companies.)

These are the kinds of questions beginning to be addressed by business users of advanced international data transmission facilities. The present lack of sound, definitive answers adds to the persistent concern about governments' regulation of this field of business operations. A U.S. automotive executive summed up: "The tempest-in-a-teapot could quickly escalate to hurricane proportions."

Broadening Restrictions

Another source of business uneasiness is the possibility that governments will not limit their restrictions to electronically transmitted data. If a country were to restrict international data transmission for security reasons, it cannot be expected to leave a large loophole in its security precautions by limiting such restrictions to data sent out of the country via electronic media. An example is immediately available. The United States prohibits the shipment of selected technology and the transmission of certain technological data to some countries for national security reasons. Such prohibitions apply to all means of transferring such data, not just to electronic transmission.

In the possibility of taxation of information transmission, international firms cannot expect governments to leave loopholes that would permit companies to avoid taxes by changing their means of transmitting data. If governments (and that is a big if, according to many interviewed executives) can develop effective methods for placing values on internationally transmitted data and for taxing that data, companies can expect new taxes to apply to all data transmission. Governments are not going to let companies avoid paying taxes on exported data by simply sending them via courier or through the mails.

Some countries, as mentioned before, already apply all or part of their data-protection laws to manually maintained and processed data as well as to those that are electronically stored and processed. Of greater concern to a number of survey participants is a clause in the Council of Europe convention on data protection, now in the process of final ratification. In its title and throughout its text, the convention concerns itself explicitly with the automatic processing of data. Yet specific articles may apply to manually processed data as well. (See Article 3, Section c in Appendix B, page 21.) If governments should extend their privacy and other restrictive laws and regulations to all forms of international data transmission and couple this with increased monitoring for compliance, the impact on international business operations for private multinational companies could be seriously inhibiting.

Several interviewed executives pointed out that rapid advances in technology and the anticipated growth in the uses of advanced telecommunications and data processing necessary for international firms to compete successfully, make new government restrictions less likely. The Swedish experience in regulating data bases was cited as an example. As the ownership and use of computers (including personal computers) spread in Sweden, the number of small data bases technically subject to government registration and control grew. The size of the staff of the regulatory government agency did not keep up, and priorities had to be set. Any effort on the part of the agency to widen its scope of supervision to all segments of the rapidly expanding electronic-data community would have foundered on the rocks of budget and staff shortages. The results are an apparent narrowing of the application of the regulations from what was originally envisioned, and a more explicit definition of objectives to reflect the realities of the present situation. Thus, the Swedish government's original goals may be achieved more successfully.

Governments' Concerns

The present and anticipated growth of data-processing and international-telecommunications systems is a matter of uneasy concern for governments as well as for businesses. As the recent history of technology exchange shows, governments and state-owned companies tend to seek the highest level of technology in fields in which they operate.[1] The same is generally true for PTT's and other state-owned firms in the fields of EDP and telecommunications. Yet, there appears to be one difference. Seeking the most modern jet airplanes for the government-owned airline or the most advanced power-transmission systems for government-owned utilities is not only welcomed, but is usually greeted with applause by officials and citizens alike. In acquiring the most advanced technology for data processing and international data transmission, the government's welcome and applause are frequently tempered by anxiety and concern. The more advanced and successful in terms of speed and efficiency the technolgy is, the more marvelous and desirable it may seem to government officials, but also the more concern it generates for its possible impact on other government interests.

[1]Relevant studies include: James R. Basche, Jr., and Michael G. Duerr, *International Transfer of Technology: A Worldwide Survey of Chief Executives,* The Conference Board, Report No. 671, 1975; and James R. Basche, Jr., *Technology Imports into the United States.* The Conference Board, Research Bulletin No. 129, 1983.

Governments' concerns stem from several factors. The first is the desire, already mentioned, to protect the privacy of their citizens. Even governments that do not ordinarily protect citizens from domestic searching into private affairs may want to protect them against prying from foreign sources.

Another factor is national security. If governments find that national data bases—whether government-controlled or privately controlled—can be entered from foreign access points, or if they find that—for any reasons—they must store some of their economic or military information abroad, they may feel they have become less secure.

Regulations of international data transmission resulting from security concerns can have important effects on international firms. For example, security reasons can be used to justify intrusive monitoring of incoming and outgoing international business communications. An article from Taipei in *The Asian Wall Street Journal Weekly* of January 30, 1984, shows how pervasive, if not chilling, such intrusive monitoring can be. The article reported a government requirement in Taiwan that multinational banks and companies using high-speed international data transmission facilities hire security officers. These officers are to be approved by the government's security agency, and their job is to monitor outgoing messages to prevent security breaches. The security concern of a government in such a case increases the unease of many firms about doing business in a country with such restrictions on international data transmission.

Another factor causing concern to some governments is the perceived loss of cultural independence. As information of all kinds (business, social, political, economic, entertainment, literary) can be, and sometimes is, readily transmitted across borders, a homogenization of culture is foreseen and the loss of national uniqueness is feared. If national security or cultural independence are abridged in any way, governments may believe their sovereignty and political existence are also threatened.

Finally, governments are concerned that unrestricted international data transmission could lead to a loss of control over their own economic development and growth. They see that rapid technological developments in EDP and telecommunications can lead to centralized decision making and control in private companies. They fear that this centralization process may, in turn, lead to more decisions affecting their economic development being made by multinational companies acting by remote control from areas outside their political borders and without reference to their political pressures and controls.

The basic concern of governments is clear: On the one hand, advanced technology is useful, needed and desired; on the other, this technology ignores national borders and appears to be a potential threat to the sovereignty of nations and their governments as they presently exist.

Business leaders, too, are aware of this as a legitimate government concern—even if they do not recognize it as real. Real or not, however, it can have serious future effects on international data transmission beyond the current privacy and technical and emerging economic concerns of governments. A U.S. survey participant wrote: "As information is more and more recognized and managed as a resource, the control of information, its location and its use—that until now have been futuristic speculation—could quickly become political issues."

IV. The Impact on Managing International Business

The general impact of government regulation of international data transmission on the management of international business operations has been minimal up to the present time. Although unevenly distributed among industries, it is slowly growing for all. As shown in this survey, a substantial majority of business users of international data transmission facilities regard such government regulations more as a nuisance than as a determining factor. None has yet made foreign investment decisions based mainly on the data transmission issue. For an important minority of international business firms, however, the impact of such regulations has been real; for a few, it has been significant enough to result in some changes in their costs and in their way of conducting business operations.

The problems and concerns stemming from government regulation of international data transmission are not going to disappear. In fact, a large number of participants in this study expect these problems to grow steadily. To support their view, they point to the increasing number of countries with data-protection laws, the technical restrictions on this field imposed in Brazil and elsewhere, and the discussions in some countries about taxing or applying other economic restraints on data sent across borders.

Furthermore, they point out that regulation of this field is already extending beyond national governments to international organizations. The OECD, the Council of Europe, and the UN Centre on Transnational Corporations (UNCTC) have already undertaken studies and, in some instances, have made recommendations to their member states of steps to be taken to regulate international data transmission. More activity can be expected from these and other organizations. UNCTC is currently considering a proposal for expanding its program in this area. And the subject is on the agendas of the European Community and the Intergovernmental Bureau for Informatics (IBI). The IBI was created under the auspices of the United Nations and UNESCO (the United Nations Educational, Scientific and Cultural Organization); it has a broad mandate to assist member governments (largely among developing countries) in the development of informatics policies and regulations. In turn, it has assisted related regional groups in Latin America and Africa to propose recommendations in this area. These could then be a prelude to new national regulations in those regions in the future.

In addition to spreading geographically, the regulation of international data transmission is expanding in coverage. During the first decade of new regulatory concern, which began when the Swedish government passed its data protection law in 1973, government emphasis has been on the protection of privacy for their citizens. Also of concern, but perhaps discussed less openly in international forums were national-security concerns about international data transmission. More recently, discussions have spread to economic, cultural and political issues as well. In the view of many study participants, companies carrying on international business would be unwise to expect governments to retract these expanding interests and to concentrate once more on only privacy or privacy plus security concerns.

The impact of regulation in this area has fallen unevenly on industries. Data-processing and telecommunications-equipment manufacturers and service providers have been affected more than many general users of the equipment and services they provide. Banks and other financial services companies, as well as some advertising, publishing and direct-mail promotion firms, all occasionally at least require the transmission of data linked to individual names. These companies have felt the impact of privacy legislation far more than manufacturing firms, whose main use of international data-transmission facilities may be to send monthly aggregated financial or production reports back to their headquarters in another country. The differences between service and nonservice industries have been mentioned before. Even within the manufacturing community there are differences in the impact of regulations, depending on the kinds of data-transmission facilities used and the extent of their use.

It is important to recognize the differences between the providers of data-processing and telecommunications equipment and services and the larger number of general users, as well as the differences among the users. However, it is equally important to recognize that some restrictions and obstacles to international data transmission confront all international firms that must send business data across national borders. (One example is incompatible national standards for equipment.) Widely shared business concerns

can be expected to grow as the number of regulations increase and as the geographical and subject areas covered by them expand to embrace more business users in all industries.

One effect of the regulation of international data transmission has been the education of some international business executives about the problems in this area. Education, in turn, has led a number of companies, including some that have not yet encountered any problems, to monitor developments, either separately or jointly, through appropriate international business organizations. If the regulation of international data transmission continues as a "growth industry," as foreseen by many survey participants, more companies may find themselves devoting some of their efforts to both educational and monitoring activities.

With expanding government interests in and regulations of international data transmission, companies in international business need to recognize the legitimate concerns on the part of governments for national security, economic development, and the protection of individual citizens' rights. Recognizing these concerns, business firms should, according to several study participants, exercise some self-restraint in their use of international data transmission as an operational tool. According to these respondents, firms should transmit internationally only the information that they really need and use; they should not be seduced by the enlarged capacity of the facilities or persuaded by staff members, who find certain information merely interesting, into sending across national borders many bits of information that will not contribute to decision making and the successful international operations of the firm. This kind of self-restraint would permit firms to make strong arguments to governments that the only data being sent are useful and necessary to efficient company operations. This approach may generate more reasonable attitudes on the part of the many government regulatory authorities dealing with this issue.

The other side of the coin, the same participants suggest, involves the responsibility of governments and their regulatory agencies. They need to recognize that a basic concern of business managers is to be able to transfer data speedily and completely from the place where they are stored to the place where they are needed and used. In a world where information has assumed enormous importance to industrial production and distribution of all kinds of goods and services, the availability of the right information at the right time in the right place to be most effectively used is essential to meet the competitive demands confronting all companies.

Both international business and national governments have roles to play, according to participants in this study, if the anticipated continuing regulation of international data transmission is to have a positive, rather than a negative, impact on international business operations and is to benefit both the companies and the governments.

Appendix A

Excerpts from the Council of the Organisation for Economic Co-operation and Development: Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23rd September, 1980)[1]

The Council

* * *

Recommends

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September, 1980. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Part One
General

* * *

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

   a) as few as possible, and

   b) made known to the public.

5. In the particular case of Federal countries, the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

Part Two
Basic Principles of National Application

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[1]Organisation for Economic Co-operation and Development, C (80) 58 (final), October 1, 1980.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

    a) with the consent of the data subject; or
    b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

    a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

    b) to have communicated to him, data relating to him

        i) within a reasonable time;

        ii) at a charge, if any, that is not excessive;

        iii) in a reasonable manner; and

        iv) in a form that is readily intelligible to him;

    c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

    d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Part Three
Basic Principles of International Application: Free Flow and Legitimate Restrictions

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

* * *

Appendix B

Excerpts from the Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (28 January, 1981)[1]

* * *

Chapter 1
General Provisions

Article 1

Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

* * *

Article 3

Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c. that it will also apply this convention to personal data files which are not processed automatically.

* * *

Chapter 2
Basic Principles for Data Protection

Article 4

Duties of the Parties

1. Each party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5

Quality of data

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6

Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data con-

[1]Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," *European Treaty Series*, No. 108 (Strasbourg, 1981).

cerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7

Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8

Additional safeguards for the data subject

Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9

Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c, and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10

Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

* * *

Chapter 3
Transborder Data Flows

Article 12

Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each party shall be entitled to derogate from the provisions of paragraph 2:

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

• • •

Chapter 7
Final Clauses

Article 22

Entry into force

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23

Accession by non-member States

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

• • •

Article 25

Reservations

No reservation may be made in respect of the provisions of this convention.

Selected Bibliography

Eger, John M. "The International Information War," *Computerworld Extra*! March 18, 1981.

Freese, Jan, and Rossitor W. Langhorne. "Transborder Data Flow: Should It Be Regulated? Pro and Con." *Computerworld,* October 30, 1978.

Intergovernmental Bureau for Informatics, *Transborder Data Flow Policies.* Papers presented at the IBI Conference on Transborder Data Flow Policies, Rome, New York: Unipub for IBI, June, 1980.

Linowes, David F. "Communications Satellites: Their Impact on the CPA." *Journal of Accountancy,* September, 1981.

Organization for Economic Cooperation and Development, Directorate for Science, Technology and Industry. *Transborder Data Flows in International Enterprises: Based on Results of a Joint BIAC/OECD, Survey and Interviews with Firms.* Paris: OECD, October, 1983.

Robinson, Peter. "Transborder Data Flow." (A speech to the Ottawa Chapter of the Canadian Information Processing Society). January, 1983.

Special Secretariat of Informatics of the National Security Council of the Presidency of the Republic of Brazil. *Transborder Data Flows and Brazil: Brazilian Case Study.* New York: U.N. Centre on Transnational Corporations, 1983.

Spero, Joan Edelman. "Information: The Policy Void," *Foreign Policy,* Fall, 1982.

United Nations Centre on Transnational Corporations. *Transnational Corporations and Transborder Data Flows: A Technical Paper.* New York, 1982.

USA-BIAC Committee on International Information Flows. *The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data: Implications for U.S. Business,* New York: January, 1982.

U.S. House of Representatives. *International Data Flow.* Hearings before the Government Information and Individual Rights Subcommittee of the Committee on Government Operations, Ninety-Sixth Congress, Second Session), March and April, 1980. Washington, D.C.: Government Printing Office.

U.S. Senate, Committee on Commerce, Science, and Transportation. *Long-Range Goals in International Telecommunications and Information: An Outline for United States Policy,* (S. PRT. 98-22), March 1983. Washington, D.C.: U.S. Government Printing Office.

Yurow, Jane H., ed. *Issues in International Telecommunications Policy: A Source Book,* Conference Edition. Washington, D.C.: The Federal Communications Bar Association and The International Law Institute of Georgetown University, 1983.